ISSN: 2321-7782 (Online)
Volume 3, Issue 2, February 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Key Generation Policy for Durable Storage in Cloud

P.Madhubala[1]
Research Scholar, Computer science,
Mother Teresa Women's University,
Kodaikanal, TN, India

P.Thangaraj[2]
HOD, Department of CSE,
Bannari Amman Institute of Technology,
Sathiyamangalam, TN, India

Abstract: ***Storage is at the bouncing core of any cloud service, and cloud storage is one of the broadest and fastest growing categories of cloud services. Security is one of the top concerns have with Cloud Computing. In the past, many businesses felt comfortable allowing the cloud provider to manage encryption keys, believing that security risks could be managed through contracts, controls and audits. Over time it has become ostensible, however, that cloud providers cannot honor such assurances when responding to requests for information from the user. To make the data secure from various attacks and for the integrity of data encryption, data should be done before it is transmitted or stored. While encryption enables access control to our data stored in cloud, poor key management and storage can worsen the data integrity. Encryption key management is an exhausting challenge at the remarkable appeal. In this paper we suggested a solution for durable key generation strategy for key management to retain robust data integrity.***

Keywords: Cloud, Encryption, integrity, key, security.

I. INTRODUCTION

The National Institute of Standards and Technology (NIST) puts it this way: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST also categorizes cloud computing into three "as a service" offerings, namely infrastructure, platforms and software. Also in this Cloud terminology, the term "as a service "refers the ability to use something over the internet on as-needed basis. This computing model delivers a single working platform and contains the mixed topographies of distributed, internet and grid computing. Also it provides the framework for outsourcing to exist. Cloud platforms are driving down the costs of engineering by offering robust enterprise architectures as-a-service. At the same time, cloud infrastructure is driving down the costs of scalable storage and computing power by providing those things as a service. Cloud Computing has several advantages such as: One can access applications as utilities, over the Internet, and manipulate and configure the application online at any time. It does not require installing a specific piece of software to access or manipulating cloud application.

Although Cloud Computing is a great innovation in the world of computing, there also exist downsides of cloud computing.one of the biggest concern about cloud computing is data management and infrastructure management. Because in cloud, data storage is provided by third-party, it is always a risk to handover the sensitive information to such providers. Some of the security services are also provided by the third-party security services. The data in provider's room could create difference of opinion about the protection of data. As many businesses plan to manage their IT infrastructure in the cloud, it's important to protect both cloud and on-premise infrastructure to ensure that all corporate assets remain secure. To keep an organization's infrastructure and business secure, organizations must enforce the appropriate levels of protection both on premise and in the cloud. The issue of cloud security is much more complex than simply "is the cloud secure or not". Whether an organization provides cloud services or purchases services from a cloud provider, it needs to be properly encrypted. The most

secure techniques use a mathematical algorithm and a verifiable value known as a 'key'. The selected key is input to encryption and is integral to the changing of data. The exact same key must be input to enable decryption of the data.

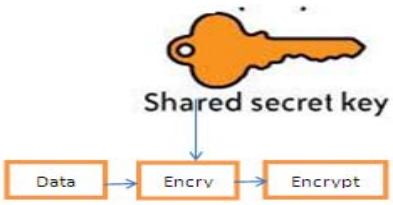


Figure 1: Basic Encryption

The two components required to encrypt data are algorithm and a key. In Symmetric encryption same key is used for encryption and decryption. In asymmetric encryption, the key used for decryption is different from the key used for encryption. A key management solution (KMS) is an integrated approach for generating, distributing and managing cryptographic keys for devices and applications. Compared to the term key management, a key management solution is tailored to specific use-cases such as secure software update or machine-to-machine communication. In a holistic approach, it covers all aspects of security - from the secure generation of keys over the secure exchange of keys up to secure key handling and storage on the client. Thus, a key management solution includes the backend functionality for key generation, distribution, and replacement as well as the client functionality for injecting keys, storing and managing keys on devices. With the Internet of Things, key management solutions become a crucial part for the security of connected devices.

II. The Need for Key Management in The Cloud

Key management isanythingyoudowithakeyexceptencryptionanddecryptionandcoversthe creation/deletion of keys, activation/ deactivation of keys, transportation of keys, storage of keys and soon. Most Cloud service provider's provide basic key encryption schemes for protecting data or may leave it to the user to encrypt their own data. Either way, there is a need to encrypt data that is involved in the Cloud. But how do we handle the keys that are used for encryption? Where should the keys be stored and who has access to those keys? How do we recover data if keys are lost? Both encryption and key management are very important to help secure applications and data stored i n the Cloud, Especially in recent times, there has been a strong need for Cloud providers to adopt a robust key management scheme for their services. However, t here are still key management issues affecting Cloud computing.

We discuss the 3 requirements of se*cure key stores*: The key stores themselves must be protected from malicious users. If a malicious user gains access to the keys, they will then be able to access any encrypted data the key is corresponded to. Hence the key stores themselves must be protected in storage, in transit and on backup media.

» ***Access to key stores*:** Access to the key stores should be limited to the users that have the right to access data. Separation of roles should be used to help control access. The entity that uses a given key should not be the entity that stores the key.

» ***Key backup and recoverability*:** Keys need secure backup and recovery solutions. Loss of keys, although effective for destroying access to data, can be highly devastating to a business and Cloud providers need to ensure that keys aren't lost through backup and recovery mechanisms. Tim Mather states that key management in enterprises today are broken and that key management in the Cloud is a failed model that is neither effective nor scalable.

III. Today's Challenges in Key Management

While cryptography is at the root of many diverseprocedures that can offer powerful security, without appropriate management these processes can become difficult, costly, and risk-prone. The ability to accomplish security operations constructed on cryptography—such as digital signing or data encryption—be subject to squarely on the ability to

achievesuccessfully the cryptographic keys that run these processes. Key management challenges will only increase over time as cryptography is employed more broadly within an organization's IT infrastructure, driving up the number and diversity of keys to be managed. Individuals responsible for implementing cryptographic security must familiar with different approaches to key management, key management best practices, and technology alternatives for implementing those practices.

Key management is not just an operational challenge. As regulatory bodies become more aware of the importance of key management, the security and audit requirements specific to these processes are becoming more stringent. In addition to this, standards such as the OASIS Key Management Interoperability Protocol (KMIP) are maturing and will improve key management interoperability between different devices and systems. Given these trends, organizations need to consider, operational, security, and audit requirements when building a key management strategy.

While cryptography is at the root of many different processes that can provide powerful security, without proper management these processes can become complex, costly, and risk-prone. Your ability to manage security operations built on cryptography—such as digital signing or data encryption—depends squarely on your ability to manage effectively the cryptographic keys that govern these processes. Key management challenges will only increase over time as cryptography is employed more broadly within an organization's IT infrastructure, driving up the number and diversity of keys to be managed. Individuals responsible for implementing cryptographic security need to become familiar with different approaches to key management, key management best practices, and technology alternatives for implementing those practices.

IV. KEY MANAGEMENT APPROACHES

a) Key management through software native tools.

At the simplest level, we can apply the basic key management abilities native to the individual product or products being deployed. Many commercial encryption products, for example, contain software functionality to handle at least some phases of the key management lifecycle. The accent, policies, and general security properties of these key management utilities will differimmensely among products.

b) Key management using hardened devices.

To better manage risk and ensure control of the entire key lifecycle, we can use purpose-built, toughened key management devices such as hardware security modules (HSMs) to enlarge commercial and custom applications. Out-and-out cryptographic hardware enables us to create an isolated or "trusted" zone for cryptographic functions, thus overcoming the inherent weaknesses of software-based cryptography. Using aself-governing security platform for key management also creates a powerful separation between the tasks of managing the keys and managing the applications that use those keys. Separating duties to mitigate the threat of a single super-user is a key management best practice and is strongly recommended by security standards such as PCI DSS.

c) Centralized key management.

In larger scale deployments like cloud, organizations managing keys across heterogeneous applications and systems can find themselves facing inconsistent policies, different levels of protection, and escalating costs. Implementing a centralized approach to key management offers a range of benefits, including unified policies, system-wide key revocation, automated key delivery, consolidated auditing, clear separation of duties, and a single key repository to protect and back up. By adopting a more strategic, top-down approach to key management, we can exercise a greater degree of control across the organization while improving operational efficiency. Organizations implementing centralized key management must carefully consider the security properties of a system that can become an attractive target for attackers. They also must maintain a high level of availability; resilience and fail-over mechanisms are needed to ensure that the central key management process does not become a single point of failure.

While cost and ease of use are two great benefits of cloud computing [5], there are significant security concerns that need to be addressed while moving critical applications and sensitive data to public and Cloud storage.

During the last few years, data security and integrity in cloud computing has materialized as significantly majorthing.When the users put several TB of data in to cloud storage, the users do not know about the storage location of their data. It makes the difficulty of checking the integrity of data stored in cloud. Existing encrypting technologies are not giving enough guarantees for integrity management. This makes the users distrustful in moving their sensitive data to cloud.

Therefore standard encryption is in efficient when selectively sharing data with many people, since the data needs to been crypted with more focusing technique in key management to retain the data integrity.

Related Work

Deswarte et al[4] proposed a first solution for remote data integrity. He used RSA centered function to hash the entire data file for every single authentication experiment. It is ineffective for the huge data files, also need much time to compute and transfer their hash values. Caronni proposed another protocol [6], where the server has to send Message Authentication Code (MAC) of data as the response to the message instead of storing the hash of all data. The verifier sends a unique random key for the message authentication code to achieve integrity on data from any modification or deletion. Instead of storing the whole data at server specific portions of data is stored; a deterministic confirmation method is used. At enieseet al suggested a model for using homomorphic verifiable tag that is calculated as a number that is equal to two times of number of data chunks, and stores the data file and it tags on the server. Then, the client can verify that data integrity of the file Using the queried blocks and their corresponding tags and the server generates a proof of integrity [5] [6].For the dynamic data integrity verification, Wang et al. reasoned the problem of ensuring the availability and integrity of data storage in cloud computing. They exploited the homomorphic token and error rectifying codes to attain the integration of storage precision assurance and data error localization.

V. PROPOSED SYSTEM MODEL FOR KEY MANAGEMENT

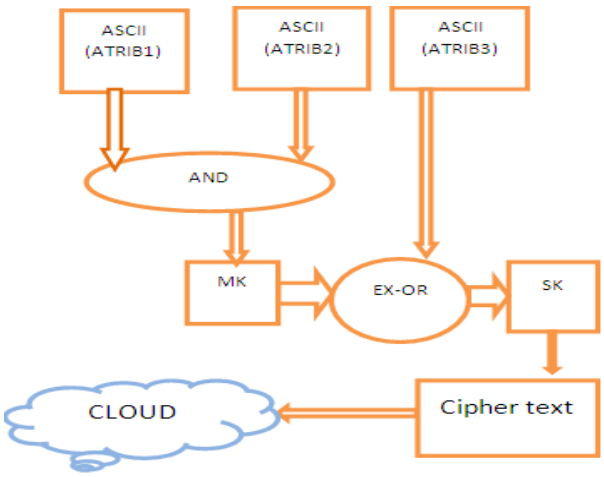
Current data security approaches focused only data security in which cryptographic solutions followed by random key generation processes, also it lacks the data integrity and robust key generation process. Computational overhead occurs at the time of the complex encryption/decryption in the server. Because cloud utilize the vast amount of request in the single time. This may cause the collision in the key of encryption which is used for secure the data. To overcome this problem we proposed data mechanism focused on the key security for the data that is being outsourced in the cloud servers and providing secure access control mechanism and data access policies to enhance the data security mechanism in the cloud.

Procedure for proposed key generation process:

1. Data and user attributes are extracted
2. Select any two attributes in random
3. Convert into ASCII values then in to binary equivalents
4. Make binary AND on two values.
5. The resultant value is master key MK
6. Take another data attribute
7. Convert it in to binary equivalent
8. Make XOR with the master key generated
9. The result is the secret key

10. Convert the text in to cipher text by hashing

11. Upload to Cloud.



When the retriever wants to retrieve the data, his request is transferred to the data owner by the third party provider. The data owner sends the secret key to the retriever in direct. With this secret key the retriever can decrypt the text obtained from cloud to get the original plain text.

VI. Conclusion

The above methodology is our proposed system. For this coding process is under developing. After completing, we will enhance this process further in future by making various analyses. The above methodology will introduce the multilevel preventive security for managing keys without any leakage.

Acknowledgement

I would like to express my sense of gratitude to DON BOSCO COLLEGE, Dharmapuri for their support and encouragement. And also I like to thank MOTHER THERESAWOMEN'S UNIVERSITY, Kodaikanal for providing me the opportunity to carry out the research work in Cloud Computing. Finally like to thank my Research Supervisor Dr.R.Thangaraj for his guidance and valuable suggestions.

References

1. M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, International Journal of Modelling and Simulation, 18(2), 1998, 112-116. (8)
2. erJ.-J.,andSaidaneA.RemoteIntegrity Checking, Proc. of ConferenceonIntegrity andInternalControl in Information Systems
3. CaronniG.andWaldvogelM.,"Establishing Trust in Distributed Storage Providers", InThirdIEEE P2P Conference, Linkoping 03, 2003.
4. Y.,Quisquat
5. GolleP.,JareckiS.andMironovI., "Cryptographic Primitives Enforcing Communication andStorageComplexity",In proc. ofFinancial Crypto 2002.Southampton, Bermuda.
6. SyamKumarP.,Subramanian R.,AnEfficient andSecureProtocolforEnsuring DataStorage SecurityinCloudComputing, IJCSI International JournalofComputerScience Issues,Vol.8, Issue6, No 1,November2011.
7. CLOUD COMPUTING MADE EASY by Cary Landis and Dan Blacharski
8. WilliamStallings,"CryptographyandNetworkSecurity:Principles &Practices", Fifth edition, Prentice Hall, ISBN-13: 78- 0136097044, 2010.
9. Chapters in Books: P.O. Bishop, Neurophysiology of binocular vision, in J.Houseman (Ed.), Handbook of physiology, 4 (New York: Springer-Verlag, 1970) 342-366. (8)
10. Theses: D.S. Chan, Theory and implementation of multidimensional discrete systems for signal processing, doctoral diss., Massachusetts Institute of Technology, Cambridge, MA, 1978. (8)
11. Proceedings Papers: EmanM.Mohamed, HatemS.Abdelkaderand SherifEl-Etriby, "DataSecurity ModelforCloudComputing",TheTwelfth International Conference onNetworks, ISBN:978-1-61208-245-5, pp66-74, 2013.

